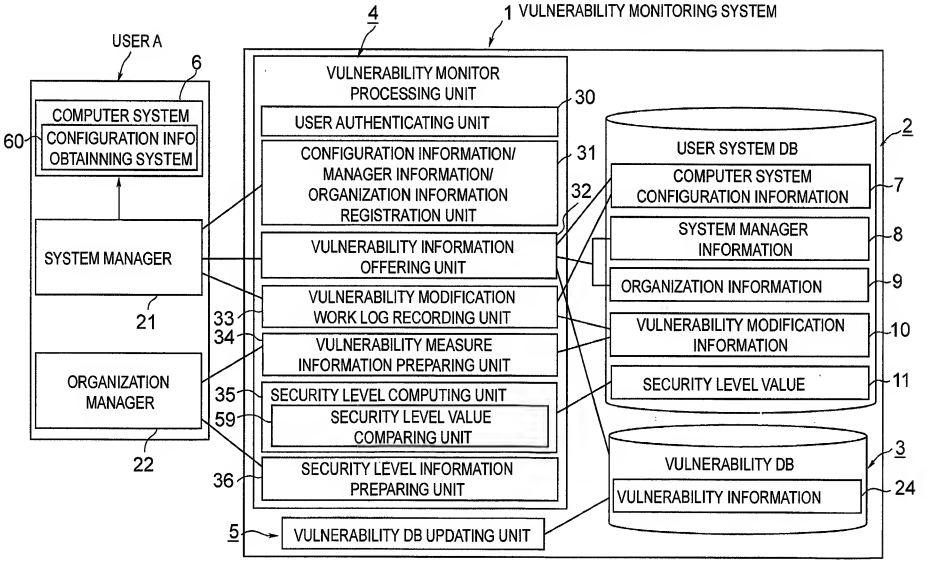

FIG. 1

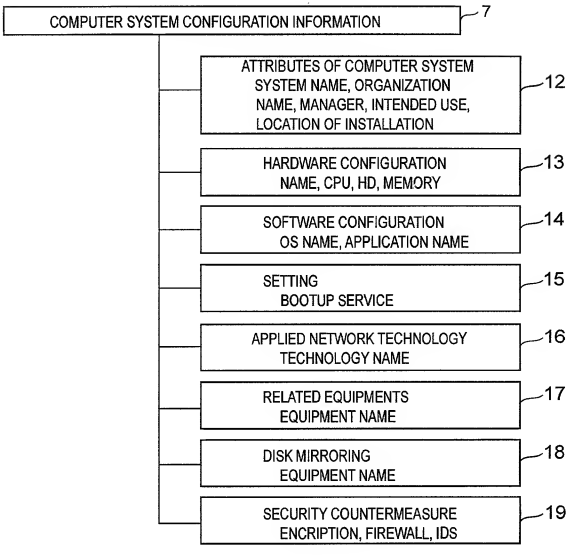
COMPUTER SYSTEM CONFIGURATION INFORMATION
7
ATTRIBUTES OF COMPUTER SYSTEM
SYSTEM NAME, ORGANIZATION
NAME, MANAGER, INTENDED USE,
LOCATION OF INSTALLATION
12
HARDWARE CONFIGURATION
NAME, CPU, HD, MEMORY
13
SOFTWARE CONFIGURATION
OS NAME, APPLICATION NAME
14
SETTING
BOOTUP SERVICE
15
APPLIED NETWORK TECHNOLOGY
TECHNOLOGY NAME
16
RELATED EQUIPMENTS
EQUIPMENT NAME
17
DISK MIRRORING
EQUIPMENT NAME
18
SECURITY COUNTERMEASURE
ENCRIPTION, FIREWALL, IDS
19

FIG. 2

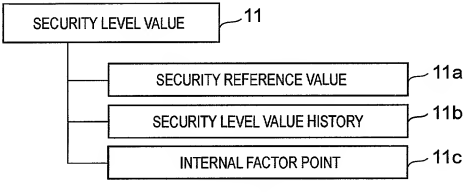
SECURITY LEVEL VALUE
11
SECURITY REFERENCE VALUE
11a
SECURITY LEVEL VALUE HISTORY
11b
INTERNAL FACTOR POINT
11c

FIG. 3

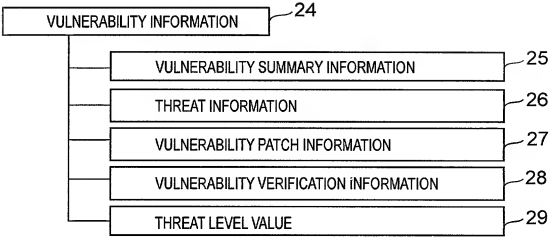
VULNERABILITY INFORMATION
24
VULNERABILITY SUMMARY INFORMATION
25
THREAT INFORMATION
26
VULNERABILITY PATCH INFORMATION
27
VULNERABILITY VERIFICATION iNFORMATION
28
THREAT LEVEL VALUE
29

FIG. 4

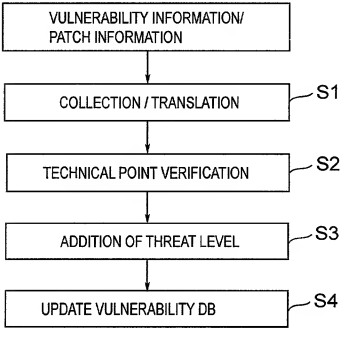
VULNERABILITY INFORMATION/
PATCH INFORMATION
COLLECTION / TRANSLATION
S1
TECHNICAL POINT VERIFICATION
S2
ADDITION OF THREAT LEVEL
S3
UPDATE VULNERABILITY DB
S4

FIG. 5

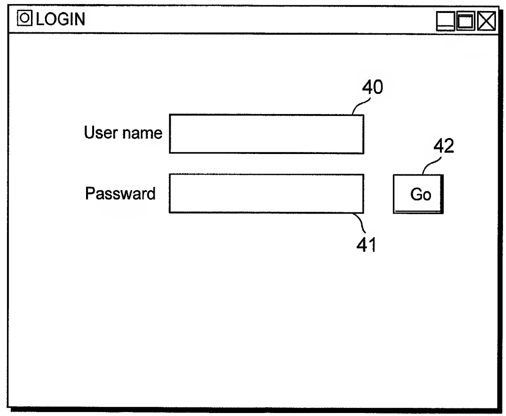

FIG. 6

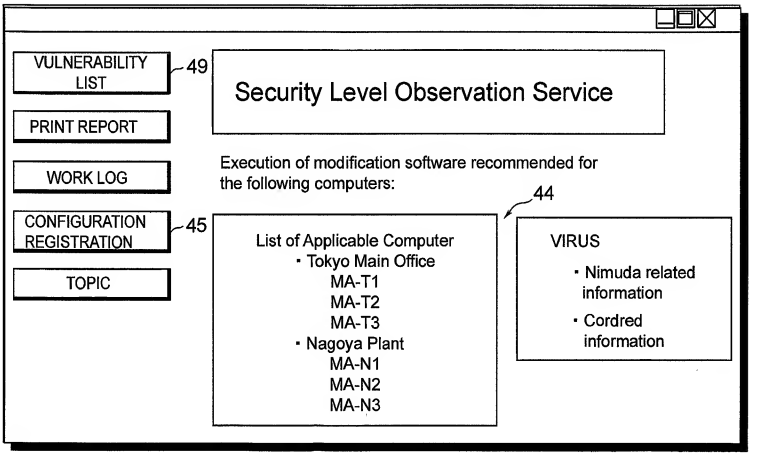

FIG. 7

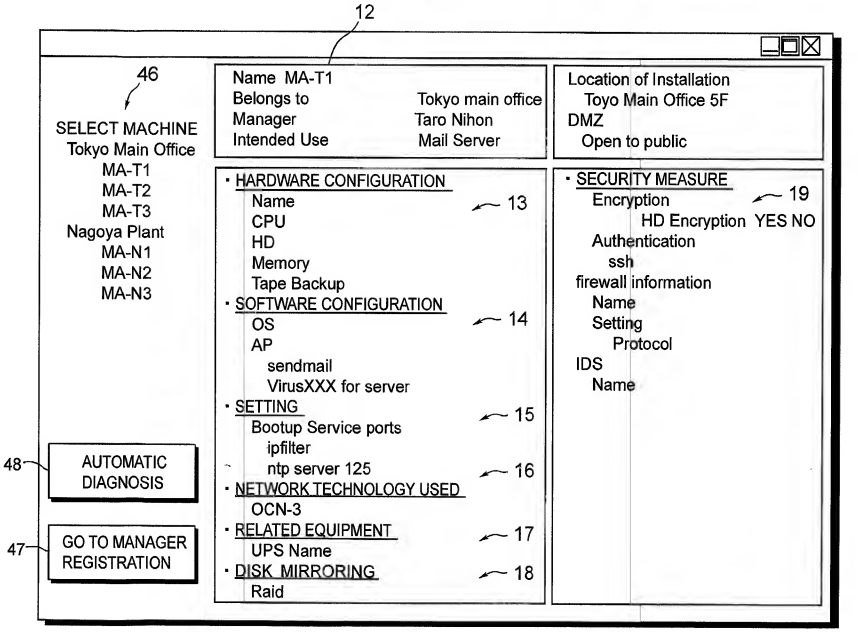
12
46
SELECT MACHINE
Tokyo Main Office
MA-T1
MA-T2
MA-T3
Nagoya Plant
MA-N1
MA-N2
MA-N3
Name MA-T1
Belongs to Tokyo main office
Manager Taro Nihon
Intended Use Mail Server
Location of Installation
Toyo Main Office 5F
DMZ
Open to public
· HARDWARE CONFIGURATION
Name
CPU
HD
Memory
Tape Backup
13
· SOFTWARE CONFIGURATION
OS
AP
sendmail
VirusXXX for server
14
· SETTING
Bootup Service ports
ipfilter
ntp server 125
15
16
· NETWORK TECHNOLOGY USED
OCN-3
· RELATED EQUIPMENT
UPS Name
17
· DISK MIRRORING
Raid
18
· SECURITY MEASURE
Encryption
HD Encryption YES NO
19
Authentication
ssh
firewall information
Name
Setting
Protocol
IDS
Name
48
AUTOMATIC DIAGNOSIS
47
GO TO MANAGER REGISTRATION

FIG. 8

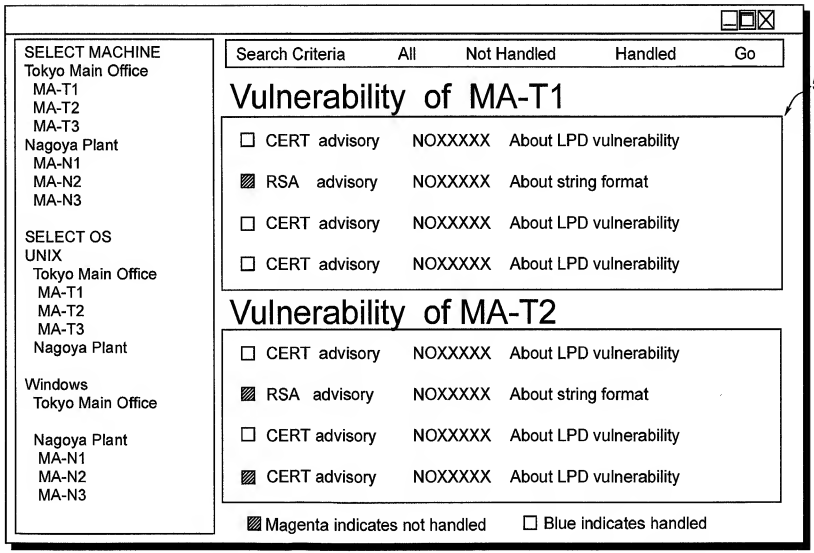

FIG. 9

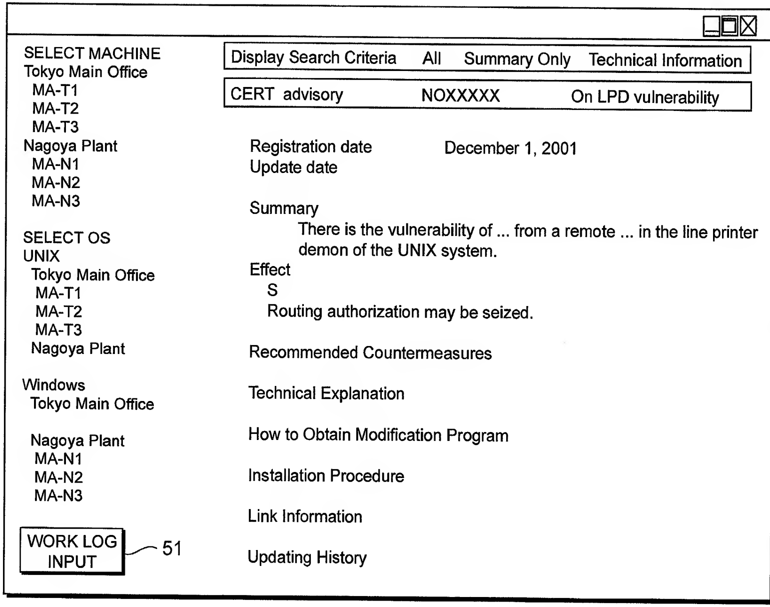
SELECT MACHINE
Tokyo Main Office
MA-T1
MA-T2
MA-T3
Nagoya Plant
MA-N1
MA-N2
MA-N3
SELECT OS
UNIX
Tokyo Main Office
MA-T1
MA-T2
MA-T3
Nagoya Plant
Windows
Tokyo Main Office
Nagoya Plant
MA-N1
MA-N2
MA-N3
WORK LOG INPUT
51
Display Search Criteria
All
Summary Only
Technical Information
CERT advisory
NOXXXXX
On LPD vulnerability
Registration date
December 1, 2001
Update date
Summary
There is the vulnerability of ... from a remote ... in the line printer demon of the UNIX system.
Effect
S
Routing authorization may be seized.
Recommended Countermeasures
Technical Explanation
How to Obtain Modification Program
Installation Procedure
Link Information
Updating History

FIG. 10

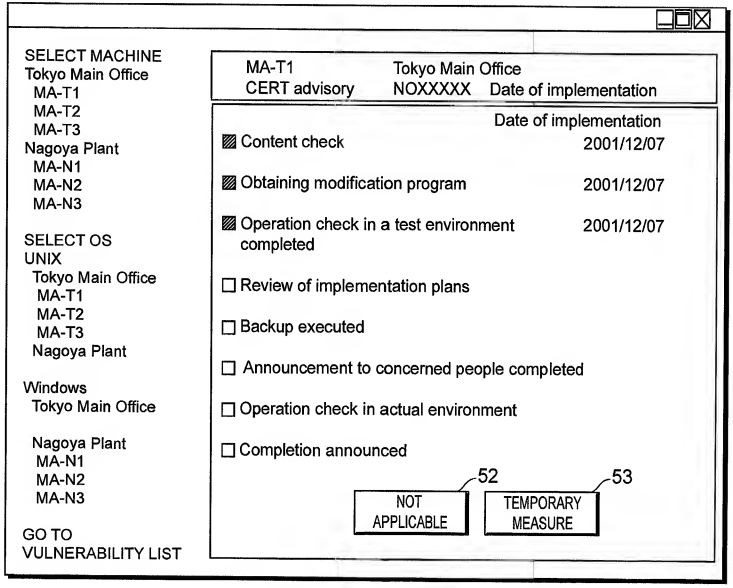

FIG. 11

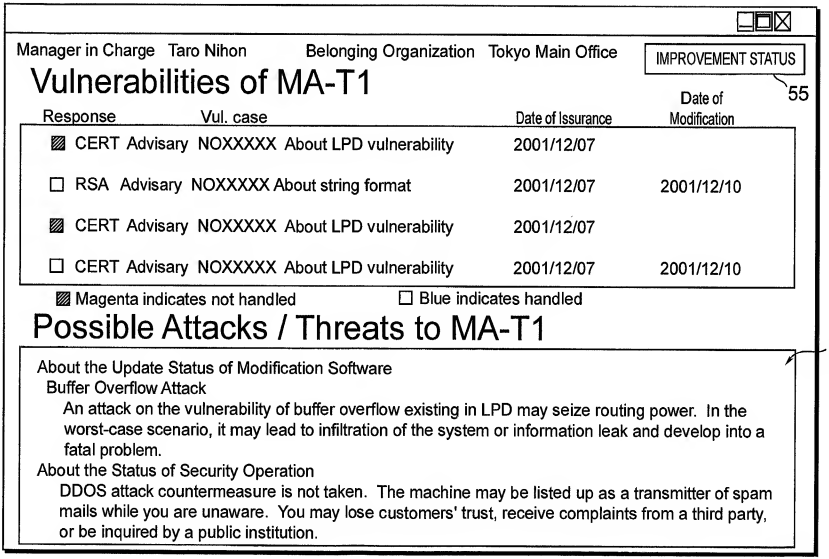
Manager in Charge Taro Nihon
Belonging Organization Tokyo Main Office
IMPROVEMENT STATUS
55
Vulnerabilities of MA-T1
Response
Vul. case
Date of Issurance
Date of Modification
CERT Advisary NOXXXXX About LPD vulnerability 2001/12/07
RSA Advisary NOXXXXX About string format 2001/12/07 2001/12/10
CERT Advisary NOXXXXX About LPD vulnerability 2001/12/07
CERT Advisary NOXXXXX About LPD vulnerability 2001/12/07 2001/12/10
Magenta indicates not handled
Blue indicates handled
Possible Attacks / Threats to MA-T1
54
About the Update Status of Modification Software
Buffer Overflow Attack
An attack on the vulnerability of buffer overflow existing in LPD may seize routing power. In the worst-case scenario, it may lead to infiltration of the system or information leak and develop into a fatal problem.
About the Status of Security Operation
DDOS attack countermeasure is not taken. The machine may be listed up as a transmitter of spam mails while you are unaware. You may lose customers' trust, receive complaints from a third party, or be inquired by a public institution.

Fig. 12

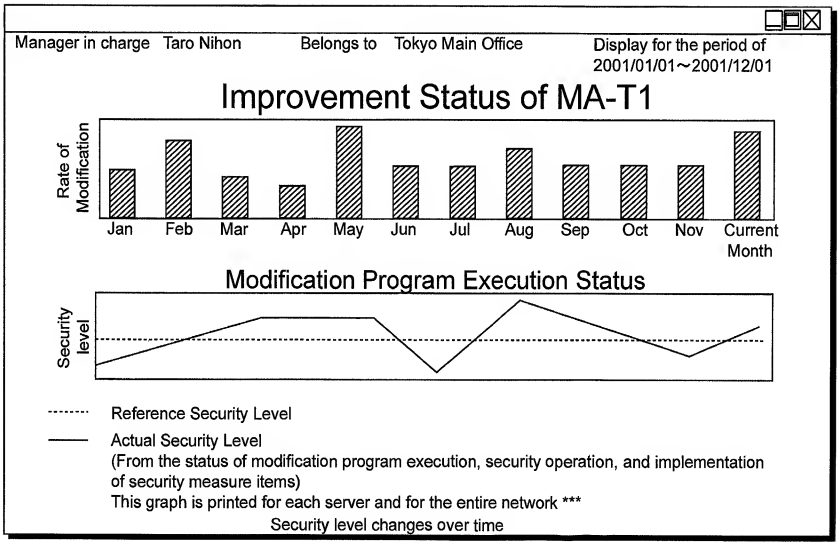
Manager in charge Taro Nihon
Belongs to Tokyo Main Office
Display for the period of
2001/01/01~2001/12/01
Improvement Status of MA-T1
Rate of Modification
Jan
Feb
Mar
Apr
May
Jun
Jul
Aug
Sep
Oct
Nov
Current Month
Modification Program Execution Status
Security level
Reference Security Level
Actual Security Level
(From the status of modification program execution, security operation, and implementation of security measure items)
This graph is printed for each server and for the entire network ***
Security level changes over time

FIG. 13

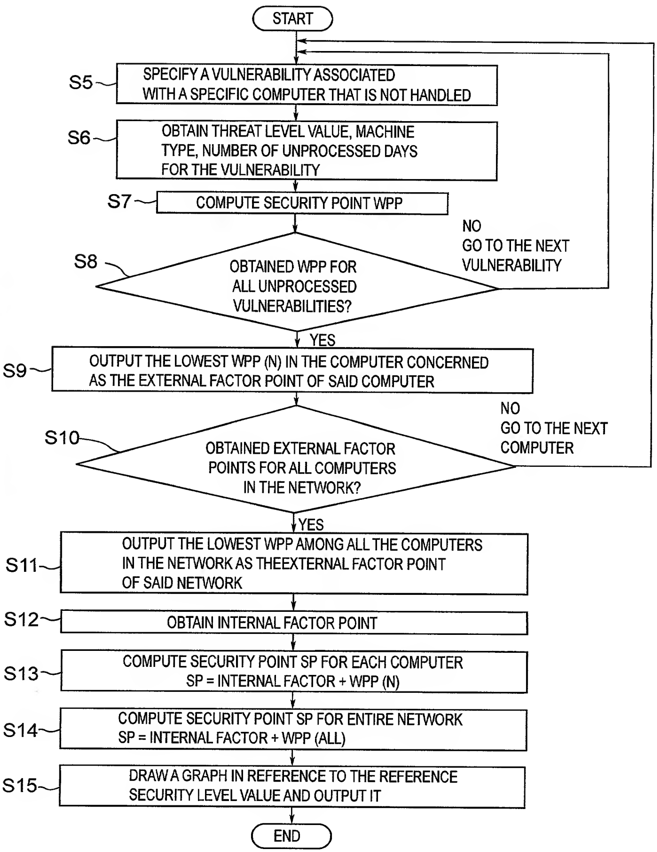
START
S5
SPECIFY A VULNERABILITY ASSOCIATED WITH A SPECIFIC COMPUTER THAT IS NOT HANDLED
S6
OBTAIN THREAT LEVEL VALUE, MACHINE TYPE, NUMBER OF UNPROCESSED DAYS FOR THE VULNERABILITY
S7
COMPUTE SECURITY POINT WPP
S8
OBTAINED WPP FOR ALL UNPROCESSED VULNERABILITIES?
NO
GO TO THE NEXT VULNERABILITY
YES
S9
OUTPUT THE LOWEST WPP (N) IN THE COMPUTER CONCERNED AS THE EXTERNAL FACTOR POINT OF SAID COMPUTER
S10
OBTAINED EXTERNAL FACTOR POINTS FOR ALL COMPUTERS IN THE NETWORK?
NO
GO TO THE NEXT COMPUTER
YES
S11
OUTPUT THE LOWEST WPP AMONG ALL THE COMPUTERS IN THE NETWORK AS THEEXTERNAL FACTOR POINT OF SAID NETWORK
S12
OBTAIN INTERNAL FACTOR POINT
S13
COMPUTE SECURITY POINT SP FOR EACH COMPUTER
SP = INTERNAL FACTOR + WPP (N)
S14
COMPUTE SECURITY POINT SP FOR ENTIRE NETWORK
SP = INTERNAL FACTOR + WPP (ALL)
S15
DRAW A GRAPH IN REFERENCE TO THE REFERENCE SECURITY LEVEL VALUE AND OUTPUT IT
END

FIG. 14